受領書

平成１１年　９月２２日
特　許　庁　長　官

識別番号　　１００００７８８６８
氏名（名称）　　河野　登夫　　殿
提出日　　平成１１年　９月２２日

以下の書類を受領しました。

項番	書類名	整理番号	受付番号	出願番号通知（事件の表示）
1	出願審査請求	12928	59900925171	特願平 4-277899
2	特許願	20565	59900925172	特願平11-269407
3	特許願	NEA0991027	59900925176	特願平11-269408
4	意見書	17435	59900925179	特願平 8-316665
5	手続補正書	17435	59900925180	特願平 8-316665
6	意見書	18329	59900925181	特願平 9-223964
7	手続補正書	18329	59900925182	特願平 9-223964
8	特許願	20391	59900925184	特願平11-269409

以　上

11-269407

【書類名】　特許願

【整理番号】　２０５６５

【提出日】　平成１１年　９月２２日

【あて先】　特許庁長官殿

【国際特許分類】　Ｈ０４Ｌ　９／１４

Ｈ０４Ｌ　９／３０

Ｇ０９Ｃ　１／００

【発明の名称】　暗号化方法，暗号通信方法及び暗号文作成装置

【請求項の数】　３

【発明者】

【住所又は居所】　大阪府箕面市粟生外院４丁目１５番３号

【氏名】　笠原　正雄

【発明者】

【住所又は居所】　京都府京都市伏見区竹田向代町１３６番地　村田機械株式会社　本社工場内

【氏名】　村上　恭通

【特許出願人】

【識別番号】　０００００６２９７

【氏名又は名称】　村田機械株式会社

【代表者】　村田　純一

【特許出願人】

【識別番号】　５９７００８６３６

【氏名又は名称】　笠原　正雄

【代理人】

【識別番号】　１００００７８８６８

【弁理士】

【氏名又は名称】　河野　登夫

【電話番号】　０６－６９４４－４１４１

【手数料の表示】

【予納台帳番号】　００１８８９

【納付金額】　２１０００

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　９８０５２８３

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号化方法，暗号通信方法及び暗号文作成装置

【特許請求の範囲】

【請求項１】　暗号化すべき平文を分割した分割平文と、該分割平文毎に準備してある複数の公開鍵から任意に選択した公開鍵とを使用して暗号文を作成する暗号化方法において、前記複数の公開鍵として、前記分割平文毎に設定した乱数項が組み込まれた複数の公開鍵を前記分割平文毎に準備しておくことを特徴とする暗号化方法。

【請求項２】　一方のエンティティ側で平文を分割した分割平文と公開鍵とを用いて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵から各分割平文について任意の公開鍵を選択し、選択した公開鍵を使用して暗号文を作成し、作成した暗号文を前記他方のエンティティへ伝送することを特徴とする暗号通信方法。

【請求項３】　暗号化すべき平文を分割した分割平文と公開鍵とを用いて暗号文を作成する装置において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵を予め格納しておく手段と、各分割平文について前記複数の公開鍵から任意の公開鍵を選択する手段と、選択した公開鍵を使用して暗号文を作成する手段とを備えることを特徴とする暗号文作成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系の暗号化方法、この暗号化方法を利用した暗号通信方法、及び、その暗号文を作成する暗号文作成装置に関する。

【０００２】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤と

して、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事，外交面で用いられてきた暗号技術が注目されている。

【０００３】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【０００４】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

【０００５】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

【０００６】

【発明が解決しようとする課題】

公開鍵暗号系の１つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をＫ分割した平文ベクトルｍ＝（m_1，m_2，・・・，m_K）と公開鍵である基数ベクトルｃ＝（c_1，c_2，・・・，c_K）とを用いて、暗号文$C=m_1 c_1+m_2 c_2+\cdots+m_K c_K$を作成し、受信者である他方のエンティティ側でその暗号文Ｃを秘密鍵を用いて平文ベクトルｍに復号して元の平文を得る暗号化形式である。

【０００７】

このような整数環上の演算を利用した積和型暗号に関して、新規な方式及び攻撃法が次々に提案されているが、特に、多くの情報を短時間で処理できるように高速復号可能な暗号化・復号の手法の開発が望まれている。そこで、本発明者等は、平文を多進法を用いて表現するようにして、高速な復号処理を可能とした積和型暗号における暗号化方法及び復号方法を提案している（特願平10－262036号，特願平10－262037号）。

【０００８】

以下、特願平10－262036号に提案した暗号化方法及び復号方法について説明する。秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：$\{b_i\}$，$\{v_i\}$，Ｐ，ｗ

・公開鍵：$\{c_i\}$

基数積$b_1 b_2 \cdots b_i$に乱数項v_iを乗じて、基数B_iを下記（１）のように与える。

$$B_i = v_i b_1 b_2 \cdots b_i \qquad \cdots (1)$$

ここで、式（１）で示される各B_iがほぼ同じ大きさになるようにv_iを設定する。但し、ｇｃｄ（v_i，b_{i-1}）＝１を満たすものとする。

【０００９】

乱数ｗを用いて、公開鍵$\{c_i\}$を下記（２）のように求める。

$$c_i \equiv w B_i \pmod{P} \qquad \cdots (2)$$

平文をＫ分割したメッセージ$\{m_i\}$と公開鍵$\{c_i\}$との積和演算により、

下記（３）のように、暗号文Ｃを得る。

$$C=m_1 c_1+m_2 c_2+\cdots+m_K c_K \quad \cdots(3)$$

【００１０】

復号処理は、以下のようにして行われる。

暗号文Ｃに対して、中間復号文Ｍを下記（４）のようにして求める。

$$M\equiv w^{-1}C \pmod{P} \quad \cdots(4)$$

この中間復号文Ｍは、具体的には式（５）として与えられるので、以下に示す逐次復号アルゴリズムによって復号できる。

$$M=m_1 b_1 v_1+m_2 b_1 b_2 v_2+\cdots+m_K b_1 b_2 \cdots b_K v_K \quad \cdots(5)$$

【００１１】

〔逐次復号アルゴリズム〕

ステップ１

$$M_1=M/b_1$$

$$m_1\equiv M_1 v_1^{-1} \pmod{b_2}$$

ステップｉ（ｉ＝２～Ｋ－１）

$$M_i=(M_{i-1}-m_{i-1} v_{i-1})/b_i$$

$$m_i\equiv M_i v_i^{-1} \pmod{b_{i+1}}$$

ステップＫ

$$M_K=(M_{K-1}-m_{K-1} v_{K-1})/b_K$$

$$m_K=M_K/v_K$$

【００１２】

元来、このような公開鍵暗号方式は、その安全性の根拠を、因数分解の困難さ，離散対数問題を解くことの困難さに置いており、それに対する攻撃も種々のものが提案されている。

【００１３】

本発明は斯かる事情に鑑みてなされたものであり、圧倒的多数の公開鍵の組合せの中から公開鍵の組を自由に選ぶことができる点に安全性の根拠を置いた新しいタイプの公開鍵暗号系の暗号化方法、この暗号化方法を利用した暗号通信方法

、及び、その暗号文を作成する暗号文作成装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】

請求項１に係る暗号化方法は、暗号化すべき平文を分割した分割平文と、該分割平文毎に準備してある複数の公開鍵から任意に選択した公開鍵とを使用して暗号文を作成する暗号化方法において、前記複数の公開鍵として、前記分割平文毎に設定した乱数項が組み込まれた複数の公開鍵を前記分割平文毎に準備しておくことを特徴とする。

【００１５】

請求項２に係る暗号通信方法は、一方のエンティティ側で平文を分割した分割平文と公開鍵とを用いて暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で元の平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵から各分割平文について任意の公開鍵を選択し、選択した公開鍵を使用して暗号文を作成し、作成した暗号文を前記他方のエンティティへ伝送することを特徴とする。

【００１６】

請求項３に係る暗号文作成装置は、暗号化すべき平文を分割した分割平文と公開鍵とを用いて暗号文を作成する装置において、前記分割平文毎に設定した乱数項が組み込まれている複数の公開鍵を予め格納しておく手段と、各分割平文について前記複数の公開鍵から任意の公開鍵を選択する手段と、選択した公開鍵を使用して暗号文を作成する手段とを備えることを特徴とする。

【００１７】

本発明では、平文を分割した分割平文毎に整数と乱数項との積からなる複数の公開鍵が予め準備されており、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文毎に選択し、選択した公開鍵を使用して暗号文を作成する。このように本発明では、公開鍵を任意に選択するので、つまり、送信者であるエンティティ側で自由に公開鍵を選択して暗号文を作成するので、その公開鍵の選択パターンが攻撃者には不明であるため、攻撃は困難となる。このように本発明

では、従来例とは異なり、その安全性の根拠を、圧倒的多数の公開鍵の組合せの中から公開鍵の組を自由に選択することに置いている。また，選択するこれらの公開鍵に乱数項を組み込ませるようにしたので、安全性をより高めることができる。

【００１８】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図１は、本発明による暗号化方式をエンティティＡ，Ｂ間の情報通信に利用した状態を示す模式図である。図１の例では、一方のエンティティＡ側で、平文ｘを暗号文Ｃに暗号化し、通信路１を介してその暗号文Ｃを他方のエンティティＢへ送信し、エンティティＢ側で、その暗号文Ｃを元の平文ｘに復号する場合を示している。

【００１９】

送信側であるエンティティＡには、平文ｘを複数の分割平文に分割する平文分割器２と、公開鍵リストを格納するデータベース10から各分割平文に対する公開鍵を選択する公開鍵選択器３と、選択した公開鍵と各分割平文とを用いて暗号文Ｃを作成する暗号化器４とが備えられている。また、受信側であるエンティティＢには、送られてきた暗号文Ｃを元の平文ｘに復号する復号器５が備えられている。この例では、公開鍵リストの発行者は受信側のエンティティＢであり、その公開鍵リストの利用者は送信側のエンティティＡである。

【００２０】

次に、具体的な手法について説明する。本発明の基本の暗号化方式は、前述した特願平10－262036号提案の方式（以下、従来方式という）の改良方式である。

【００２１】

従来方式に基づく本発明の暗号化方式の初回伝送時における中間復号文Ｍは、下記（６）で与えられる。

$$M=m_1' b_1 v_1 + m_2' b_1 b_2 v_2 + \cdots + m_K' b_1 b_2 \cdots b_K v_K \quad \cdots (6)$$

【００２２】

但し、m_i' はメッセージ（分割平文）m_i に対し、$\log_2$ Ｊビットの冗長を付加することにより、与えられたｊについてＪを法として、下記（７）が成立するように符号化されている。Ｊ＝２^g の場合、この符号化を非常に単純に実現したい場合には、m_i を上位にｇ桁だけシフトし、下位ｇ桁にｊを連接すれば良い。即ち、符号化m_i' は単に$m_i' = m_i * j$ で与えられる。

$$m_i' \equiv j \pmod{J} \quad \cdots (7)$$

【００２３】

なお、エンティティＡが選択した公開鍵を用いた一連の暗号文を送り終えるまでの一定期間内で、最初の暗号文以外ではメッセージm_i が復号されないことが考えられる。この場合、レートが若干高くなるとともに、復号過程が単純化される。

【００２４】

図２は、各分割平文毎に複数の公開鍵を予め格納しているデータベース10内の公開鍵リストを示す図である。図２において、Ｋは平文ｘの分割数（クラス数）を表す。基数積に乱数項を乗じた集合 $\{b_1\ b_2 \cdots b_i\ v_i^{(j)}\}$ が、図２に示すように、各分割平文毎（各クラス毎）にＪ個ずつの公開鍵として準備されている。

【００２５】

エンティティＢは、基数積と乱数項とのこれらの積を乱数ｗにより変換して公開する。即ち、図２に示す基数積と乱数項との積を下記（８）のように変換し、その集合 $\{c_{ij}\}$ を公開する。

$$b_1\ b_2 \cdots b_i\ v_i^{(j)}\ w \equiv c_{ij} \pmod{P} \quad \cdots (8)$$

【００２６】

エンティティＡがランダムに選択した公開鍵の組を下記（９）と表記する。この場合、エンティティＡを含む任意のエンティティにとって、J^K （≫１）通りの公開鍵選択の可能性がある。

【００２７】

【数１】

$$(c_1, j_1, c_2, j_2, \cdots, c_K, j_K) \quad \cdots (9)$$

【００２８】

エンティティＡは、上記（９）に示す選択した公開鍵の組に基づいて、$m_i' \equiv j_i \pmod{J}$とした上で、エンティティＢへの暗号文Ｃを下記（10）のように生成する。

【００２９】

【数２】

$$C = m_1' c_{1, j_1} + m_2' c_{2, j_2} + \cdots + m_K' c_{K, j_K} \quad \cdots (10)$$

【００３０】

エンティティＢは、このようにして生成される暗号文Ｃを復号するために、図２における乱数項$v_i^{(j)}$を下記（11）のように予め定めておく。但し、$w_{b,i}$，$r_i^{(j)}$は何れも乱数である。

$$v_i^{(j)} = w_{b,i} + r_i^{(j)} b_{i+1} \quad \cdots (11)$$

【００３１】

更にエンティティＢは、下記（12）を満たす$w_{b,i}^{-1}$を秘密鍵として保持する。

$$w_{b,i} \cdot w_{b,i}^{-1} \equiv 1 \pmod{b_{i+1}} \quad \cdots (12)$$

【００３２】

エンティティＢにおける復号器５での復号処理は、以下のように行われる。

中間復号文M_0は、下記（13）のように与えられる。

【００３３】

【数３】

$$M_0 = m_1' b_1 v_1^{(l_1)} + m_2' b_1 b_2 v_2^{(l_2)} + \cdots$$

$$+ m_K' b_1 b_2, \cdots b_K v_K^{(l_K)} \quad \cdots (13)$$

【００３４】

よって、下記（14）に示す逐次復号アルゴリズムによって復号できる。なお、以下においてb_{K+1}は$m_K' < b_{K+1}$を満たす乱数であるが、基数としては用いられていない。一般にステップｉにおけるj_iに対する乱数項は下記（15）のように表記している。

【００３５】

【数４】

逐次復号アルゴリズム

ステップi

$$M_1 = \frac{M_0}{b_1}$$

$$m_1' \equiv M_1 \cdot w_{b,1}^{-1} \pmod{b_2}$$

$$m_1' \equiv J_1 \pmod{J}$$

ステップi（i=2~K−1）

$$M_i = \frac{M_{i-1} - m_{i-1}' v_{i-1}^{(j_{i-1})}}{b_i}$$

$$m_i' \equiv M_i w_{b,i}^{-1} \pmod{b_{i+1}}$$

$$m_i' \equiv J_i \pmod{J}$$

ステップK

$$M_K = \frac{M_{K-1} - m_{K-1}' v_{K-1}^{(j_{K-1})}}{b_K}$$

$$m_K' \equiv M_i w_{b,K}^{-1} \pmod{b_{K+1}}$$

} ・・・(14)

$$v^{(j_i)} \quad \cdots(15)$$

【００３６】

図３は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、データベース10に予め格納されている複数の公開鍵から各分割平文について任意の公開鍵を選択する処理と、選択した公開鍵と分割平文とを用いて暗号文を作成する処理とを含むか、または、このように作成された暗号文を上述した逐次復号アルゴリズムに従って復号する処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ20は、各エンティティ側に設けられている。

【００３７】

図３において、コンピュータ20とオンライン接続する記録媒体21は、コンピュータ20の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体21には前述の如きプログラム21a が記録されている。記録媒体21から読み出されたプログラム21a がコンピュータ20を制御することにより、コンピュータ20が暗号文Ｃを作成するか、または、暗号文Ｃを元の平文ｘに復号する。

【００３８】

コンピュータ20の内部に設けられた記録媒体22は、内蔵設置される例えばハードディスクドライブまたはＲＯＭ等を用いてなり、記録媒体22には前述の如きプログラム22a が記録されている。記録媒体22から読み出されたプログラム22a がコンピュータ20を制御することにより、コンピュータ20が暗号文Ｃを作成するか、または、暗号文Ｃを元の平文ｘに復号する。

【００３９】

コンピュータ20に設けられたディスクドライブ20a に装填して使用される記録媒体23は、運搬可能な例えば光磁気ディスク，ＣＤ－ＲＯＭまたはフレキシブルディスク等を用いてなり、記録媒体23には前述の如きプログラム23a が記録されている。記録媒体23から読み出されたプログラム23a がコンピュータ20を制御することにより、コンピュータ20が暗号文Ｃを作成するか、または、暗号文Ｃを元の平文ｘに復号する。

【００４０】

以下、本発明による暗号化の数値例について説明する。

各種のパラメータをＪ＝２，Ｋ＝８，｜m_i｜＝８，Ｉ＝２とした場合の数値例を以下に示す。なお、平文m_i の偶奇により夫々$c_i^{(0)}$ 及び$c_i^{(1)}$ から選択した公開鍵をc_i と表記した。なお、以下に示す数値例は、上述した逐次復号アルゴリズムによって容易に復号できる。

【００４１】

【数５】

$$P_1 = 102910906635900382142873$$
$$w^{(1)} = 550538731465492508605 34$$
$$w^{(1)-1} = 323766708210461029448 22$$
$$P_2 = 260149294473638018394365993$$
$$w^{(2)} = 333268431806571163763006 68$$
$$w^{(2)-1} = 117709177347082312786555509$$
$$\{b_i\} = (1, 293, 271, 263, 311, 281, 269, 277, 283)$$
$$\{v_i^{(0)}\} = (1068589946674402 1506, 662589350771435 56, 19406216010482 7, 1074494359574, 3416007300, 12107042, 42345, 997)$$
$$\{v_i^{(1)}\} = (1579395796626846 3201, 565565654321135 05, 18388221377618 4, 1225119957987, 2506715466, 16419381, 37082, 997)$$
$$\{w_{b,i}\} = \{v_i^{(0)} \bmod b_{i+1}\} = \{v_i^{(1)} \bmod b_{i+1}\} = (235, 233, 210, 128, 171, 159, 241, 148)$$

【００４２】

【数６】

$$\{B_i^{(0)(1)}\}=\{w^{(1)} b_1 b_2 \cdots b_i v_i^{(0)} \bmod P_1\}$$
$$=(106858994667440215 06,$$
$$194138679776030619 08,$$
$$154091176988035782 81,$$
$$224386538915458866 86,$$
$$221856337325139267 00,$$
$$220951735759820443 58,$$
$$207880515856114276 95,$$
$$135577173653246484 239,$$
$$384837915184240271 21)$$

$$\{B_i^{(1)(1)}\}=\{w^{(1)} b_1 b_2 \cdots b_i v_i^{(1)} \bmod P_1\}$$
$$=(157939579662684632 01,$$
$$165710736716092569 65,$$
$$146007994204703381 52,$$
$$255841666063229831 43,$$
$$162801382773110488 14,$$
$$299651288238020183 19,$$
$$182043341338444435 42,$$
$$135577173653246484 239,$$
$$384837915184240271 21)$$

$$\{c_i^{(0)}\}=\{B_i^{(0)(2)}\}=\{w^{(2)} B_i^{(0)(1)} \bmod P_2\}$$
$$=(162773815812901090377734403,$$
$$930250512530326974348090 27,$$
$$622052850763178064125214 71,$$
$$259428598904157633423079 243,$$
$$217251256667441573416357 617,$$
$$467336065401598647428671 02,$$
$$214784340940908602891069 724,$$
$$102147719304960540202300 258,$$
$$898826459999238067903305 49)$$

【００４３】

【数７】

$$\{c_i^{(1)}\}=\{B_i^{(1)(2)}\}=\{w^{(2)}B_i^{(1)(1)} \bmod P_2\}$$
$$=(191272628640899272049659235,$$
$$249985745113542801003131066,$$
$$201270705789948255796606712,$$
$$465557081847493756350521 56,$$
$$246511137861367171102859869,$$
$$250687268105719102100996604,$$
$$490057626859808978959316 98,$$
$$102147719304960540202300258,$$
$$898826459999238067903305 49)$$

$$\{m_i\}=(199,188,217,237,142,254,189,249)$$

$$\{c_i\}=(191272628640899272049659235,$$
$$930250512530326974348090 27,$$
$$201270705789948255796606712,$$
$$465557081847493756350521 56,$$
$$217251256667441573416357617,$$
$$467336065401598647428671 02,$$
$$490057626859808978959316 98,$$
$$102147719304960540202300258,$$
$$898826459999238067903305 49)$$

$$C = m_1 c_1 + m_2 c_2 + \cdots + m_8 c_8$$
$$= 187678294493876349071512183003$$

【００４４】

次に、公開鍵の可能な組合せ数N_B，公開鍵リストのサイズS_C，初回伝送暗号文のレートＲ及び定常時の暗号文のレートｒ（情報記号数／暗号文長）の数値例について述べる。但し、Ｊ＝２，Ｋ＝128，$|m_i|$＝64（ビット）とし、$b_i = 2^{64} + \delta_i$（$2 \leqq i \leqq K$），$b_1 = 1$，$1 \ll \delta_i \ll 2^{64}$とする。なお、最初の暗号文のみ符号化メッセージを用いる。

【００４５】

$N_B = J^K = 2^{128} \fallingdotseq 3.40 \times 10^{38}$となる。公開鍵のサイズ$|c_i|$＝64×128＝8192（ビット）であるので、$S_C$＝8192×２×128 ≒2.097（Ｍビット）（262 ｋバイト）となる。また、最初の暗号文の符号化メッセージm_i'のサイズは64（ビット）であり、$\log_2 J = \log_2 2 = 1$である。最初の暗号文のメッセージのサイズ$|m_i|$は$|m_i'|$＝64（ビット）である。従って、最初の暗号文

のレートＲは、Ｒ＝ (63×128)／ (8192＋64＋ $\log_2$ 128)＝8064／8263＝0.976 となる。第２回目以降の定常時の暗号文のレートｒは、0.991 で与えられる。

【００４６】

ところで、Ｊ＝４，Ｋ＝64と設定した場合、他が同一の条件であるときには、夫々の値が以下のようになる。

$N_B = 4^{64} \fallingdotseq 3.40 \times 10^{38}$

S_C ＝4096×２×128 ≒1.048 （Ｍビット） （131 ｋバイト）

Ｒ＝0.968

ｒ＝0.983

【００４７】

以下、本発明の安全性について考察する。

法Ｐを秘密にしても、連続する３個の公開鍵 c_{i-1} ， c_i ， c_{i+1} が正しく与えられた場合には、特定攻撃（境隆一，村上恭通，笠原正雄：”積和型公開鍵暗号に関する二，三の考察”信学技報ISEC99, 1999 に開示の攻撃方法）によって、b_i ， b_{i+1} ，Ｐが露呈し、更に、Ｐが露呈すると連分数攻撃（H. Kuwakado, H. Tanaka：” The security of the improved knapsack cryptosystem”, IEICE Trans., Fundamental, vol. E81-A, no. 10, pp. 2184-2185, 1998 に開示の攻撃方法）によって、$v_{ij} < P^{1/2}$ となる乱数項が露呈する可能性がある。

【００４８】

ここで公開鍵｛c_i｝の位置が正当な受信者（エンティティＢ）のみが知る順序でランダムにシャッフルされているとすると、攻撃者は総当たり的に連続する３個の公開鍵を調べることになる。総当たりの回数は $_KC_2$ ・３！であり、この中に（Ｋ－２）組の正しい連続鍵｛（c_{i-1} ， c_i ， c_{i+1} ）｝が含まれている。従って正しい連続鍵の１組（c_{i-1} ， c_i ， c_{i+1} ）当たりに必要な総当たり攻撃の回数N_A は、下記（16）で与えられる。N_A 回の総当たり攻撃を試みた場合に１組の正解が期待されるので、このときに仮定される鍵系列の集合を正解集合と呼ぶ。

【００４９】

【数８】

$$N_A = \frac{{}_K C_3 \cdot 3!}{K-2} \quad \cdots (16)$$

【００５０】

本発明の暗号化方式について、「数論と組み合わせたＬＬＬ攻撃（上述の特定攻撃）によって秘密の一部が不完全な形ながら露呈すること」によって、安全性に関する下界を定量化することができる。本発明の安全性が非常に高いことは、次のような４点の根拠に基づいている。

①暗号化鍵の位置がランダムにシャッフルされているために、N_A 通りに得られた解の中から正解を決定することが困難であること。

②上位の $\{v_{ij}\}$，$\{b_i\}$ 等が露呈しても、下位の $\{v_{ij}\}$，$\{b_i\}$ 及び乱数ｗは露呈しないこと。

③上位の $\{v_{ij}\}$，$\{b_i\}$ が露呈しても、正しく順序付けることが困難であること。

④上記パラメータが露呈しても、乱数ｗが露呈しないのでメッセージは露呈しないこと。

【００５１】

以上のように，本発明の基本の暗号化方式は十分に安全であると考えられるが、多段暗号化を行うことにより、より安全性を高くした方式を構築できる。以下、この多段暗号化について説明する。

【００５２】

多段暗号化を行う場合には、基数積 $b_1\ b_2 \cdots b_i$ に対し、乱数ｗと素数Ｐとの組（ｗ，Ｐ）をＩ組選択し、下記（17-1），（17-2），・・・，（17-I）のようにＩ段にわたって乱数を乗じていくことにより、最終的に得られる $B_i^{(I)}$ を公開鍵 c_i とする。

$$b_1\ b_2 \cdots b_i\ w^{(1)} \equiv B_i^{(1)} \pmod{P_1} \quad \cdots (17\text{-}1)$$

$$B_i^{(1)}\ w^{(2)} \equiv B_i^{(2)} \pmod{P_2} \quad \cdots (17\text{-}2)$$

$$B_i^{(I-1)} w^{(I)} \equiv B_i^{(I)}, \quad (\mathrm{mod}\ P_I) \qquad \cdots (17\text{-}I)$$

【００５３】

但し、Ｉ個の素数P_1，P_2，…，P_Iについては、下記（18）の条件を満たすものとする。下記（18）は、復号を補償した上でP_iがP_{i-1}より小さいことを意味する。また、これらの素数P_1，P_2，…，P_Iは全て秘密にする。

$$P_1 < P_2 < \cdots < P_I \qquad \cdots (18)$$

【００５４】

なお、多段数Ｉを十分に大きくすること（$I > 2^{1/2} K$）により、｛b_1，b_2，…，b_i｝は露呈せず、数論的に安全な公開鍵の集合を構成することが可能である。この理由については後述する。

【００５５】

Ｉ段の多段暗号化を実施した場合、（Ｉ＋２）個の公開鍵の順序が正しく与えられると、上述の特定攻撃により、｛b_i｝の一部と｛P_i｝とが露呈する。この場合、正解集合のサイズ、即ち、正しい連続鍵の１組（c_{i-I}，…，c_i，c_{i+1}）当たりに必要とされる総当たり攻撃の回数N_Aは、下記（19）で与えられる。

【００５６】

【数９】

$$N_A = \frac{{}_K C_{I+2} \cdot (I+2)!}{K-I-1} \quad \cdots (19)$$

【００５７】

次に、このような多段暗号化における数値例について説明する。各種のパラメータをＪ＝２，Ｋ＝64，｜m_i｜＝64，Ｉ＝８とした場合における公開鍵の可能な組合せ数N_B，Ｉ段の多段暗号化を行った場合の正解集合のサイズN_A，第２回以降の定常時の暗号文のレートｒ及び公開鍵リストのサイズS_Cは以下のようになる。

【００５８】

【数１０】

$$N_B = 2^{64} \fallingdotseq 1.84 \times 10^{19}$$

$$N_A = \frac{{}_{64}C_{10} \times 10!}{64-8-1} \fallingdotseq 1.32 \times 10^{18}$$

$$r = \frac{64 \times 64}{64 \times 64 + 7 \times (64+6) + \log_2 64}$$

$$= 0.892$$

$$S_C = 2 \times 70 \times (4096 + 7 \times 70)$$

$$= 587\text{kビット} = 73.4\text{kバイト}$$

【００５９】

次に、情報理論的安全性に関する平文分割数Ｋと多段暗号化の段数Ｉとの関係について考察する。本発明では、以下に述べるような理由により、$I > 2^{1/2} K$を満たすようにする。

【００６０】

基数｛b_i｝の唯一つの要素でも露呈した場合には、本発明の暗号化方式の安全性が損なわれると仮定する。この仮定は、非常に安全側に立った仮定である。Ｉ個の法P_1，P_2，…，P_Iは上記（18）の条件を満たし、Ｊ＝２とする。また、符号化メッセージ長を｜m′｜とし、各P_iのサイズを｜P_i｜とする。この場合に下記（20）が成り立つ。

【００６１】

【数１１】

$$|P_I| = |P_1| + (I-1)|m'| + \log_2 K \quad \cdots (20)$$

【００６２】

各公開鍵のサイズを等しく｜c_i｜とした場合、これらは全部でＪＫ＝２Ｋ個公開されているので、それらを全て合わせたサイズは、$\log_2 K$を無視すると、下記（21）のようになる。

【００６３】

【数１２】

$$2K|c_1|=2K|P_I|$$
$$=2[K|m'|+(I-1)|m'|]K \quad \cdots(21)$$

【００６４】

一方、未知の量としてのP_1～P_I及び$w^{(1)}$～$w^{(I)}$までのサイズの和は、下記（22）のようになる。

【００６５】

【数１３】

$$|P_1|+|P_2|+\cdots|P_I|$$
$$+|w^{(1)}|+|w^{(2)}|+\cdots|w^{(I)}|$$
$$=2[IK|m'|+\frac{(I-1)I}{2}|m'|] \quad \cdots(22)$$

【００６６】

従って、下記（23）即ち下記（24）の条件を満たすようにＩを設定した場合には、公開情報量よりも未知情報量が大きくなり、解読が不可能であることは明らかである。この下記（24）の条件は、近似的にＩ＞$2^{1/2}$ Ｋである。

【００６７】

【数１４】

$$2[IK|m'|+\frac{(I-1)I}{2}|m'|]$$
$$>2[K|m'|+(I-1)|m'|]K \quad \cdots(23)$$
$$(I-1)I>2(K^2-K) \quad \cdots(24)$$

【００６８】

よって、平文分割数Ｋと多段暗号化の段数Ｉとの間にＩ＞$2^{1/2}$ Ｋの関係がある場合に、｛P_i｝，｛$w^{(i)}$｝は露呈されず、｛b_1 b_2 … b_i v_i｝が完全に秘匿されるので、極めて安全性が高い。

【００６９】

また、Ｉ＞Ｋである場合、｛P_i｝，｛$w^{(i)}$｝，｛$v^{(i)}$｝の全てが露呈することはないことを全く同様に示すことができる。

【００７０】

以下、中国人の剰余定理を応用した本発明の変形方式について説明する。ここでは記号の煩雑さを避けるために、Ｐに関連する基数をb_i'と表記する。クラスｉに属する基数積と乱数項との積の１組を$B_i^{(j)}=b_1 b_2 \cdots b_i^{(j)} v_i^{(j)}$，$B_i^{(j)\prime}=b_1' b_2' \cdots b_i^{(j)\prime} v_i^{(j)\prime}$とする。素数Ｐによる余りが$B_i^{(j)}$，素数Ｑによる余りが$B_i^{(j)\prime}$となるような最小の整数を$D_i^{(j)}$とする。更に、$D_i^{(j)}$を乱数ｗによって下記（25）のように変換し、｛$c_i^{(j)}$｝をクラスｉの公開鍵として公開する。

$$D_i^{(j)} w \equiv c_i^{(j)} \pmod{PQ} \quad \cdots (25)$$

【００７１】

中間復号文M_P，M_Qは、下記（26），（27）のようになる。但し、メッセージm_iはクラスｉの何れの公開鍵を用いて暗号化したかを示すために、上式に見られるようにm_i'に符号化しているものとする。このような中間復号文M_Pにおけるメッセージ｛m_i｝，中間復号文M_Qにおけるメッセージ｛m_i'｝の復号法は、前述した基本方式の逐次復号アルゴリズムと同様である。

【００７２】

【数１５】

$$M_P = m_1' B_1(I_1) + m_2' B_2(I_2) + \cdots + m_K' B_K(I_K) \quad \cdots (26)$$

$$M_Q = m_1' B_1(I_1)' + m_2' B_2(I_2)' + \cdots + m_K' B_K(I_K)' \quad \cdots (27)$$

【００７３】

【発明の効果】

以上詳述したように、本発明では、各分割平文毎に設定した乱数項を組み込ん

だ複数の公開鍵を予め準備しておき、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文について選択し、選択した公開鍵を使用して暗号文を作成するようにしたので、その公開鍵の選択のパターンが攻撃者には不明であって、攻撃を受けにくく、安全性を向上することができる。従来の公開鍵暗号方式とは異なり、本発明ではその安全性の根拠を、多数の公開鍵から所望の公開鍵の組を自由に選択できること、言い換えれば、その公開鍵選択の組合せの数の多さに置いており、公開鍵暗号方式の発展及び実用化を図る上で、本発明は大いに寄与できる。

【００７４】

（付記）

なお、以上の説明に対して更に以下の項を開示する。

（１）　請求項１記載の暗号化方法であって、前記分割平文と選択した公開鍵とによる複数の積を加算した形式で暗号文を作成する暗号化方法。

（２）　暗号化すべき平文を分割した分割平文と公開鍵とを用い、前記公開鍵に複数の乱数を多段化演算した演算結果を利用して積和型の暗号文を作成する暗号化方法において、前記平文の分割数Ｋと前記多段化演算の段数Ｉとに関してＩ＞$2^{1/2}$ Ｋの関係を満たす暗号化方法。

（３）　複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項１または第（１），（２）項の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から元の平文を復号する復号器とを備える暗号通信システム。

（４）　コンピュータに、暗号化すべき平文を分割した分割平文と公開鍵とを用いて暗号文を作成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、前記分割平文毎に設定された乱数項が組み込まれた複数の公開鍵から各分割平文について任意の公開鍵を選択することをコンピュータに実行させるプログラムコード手段と、選択した公開鍵を使用して暗号文を作成することをコンピュータに実行させるプログラムコード手段とを含むプログラムが記録されている記録媒体。

（５）　コンピュータに、平文を分割した分割平文と前記分割平文毎に設定された乱数項が組み込まれた複数の公開鍵から各分割平文について選択した公開鍵とを用いて作成された暗号文を復号させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体であって、選択された前記公開鍵を同定しながら前記分割平文を順次復号することをコンピュータに実行させるプログラムコード手段を含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図１】

２人のエンティティ間における情報の暗号通信状態を示す模式図である。

【図２】

データベース内の公開鍵リストを示す図である。

【図３】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

１　通信路

２　平文分割器

３　公開鍵選択器

４　暗号化器

５　復号器

10　データベース

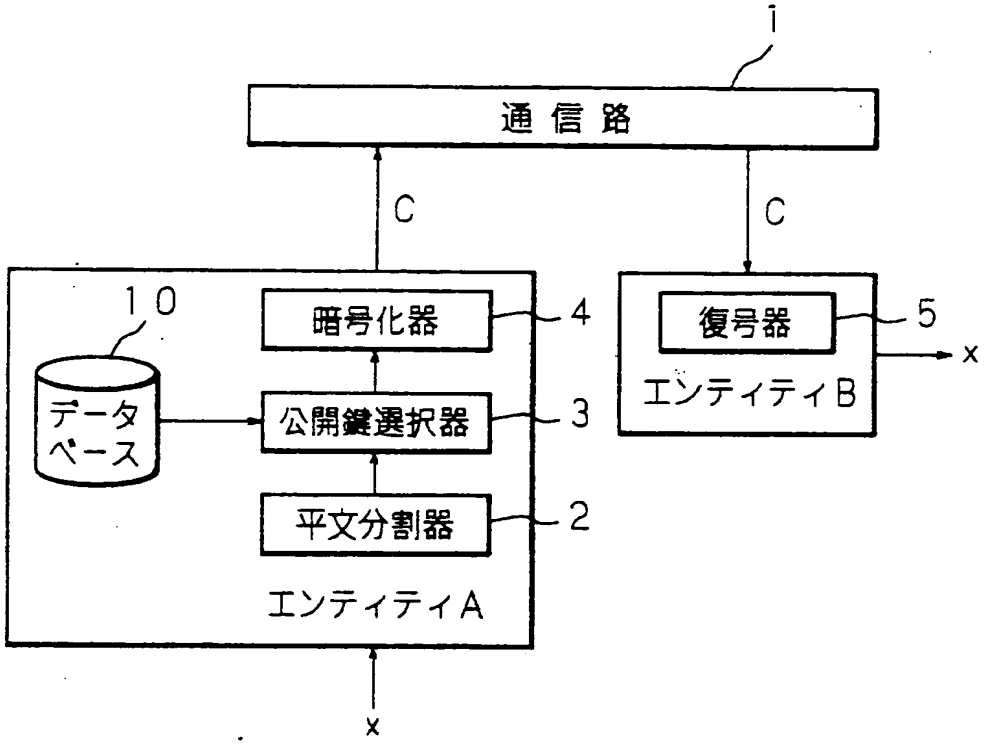
20　コンピュータ

21，22，23　記録媒体

Ａ，Ｂ　エンティティ

【書類名】　　図面

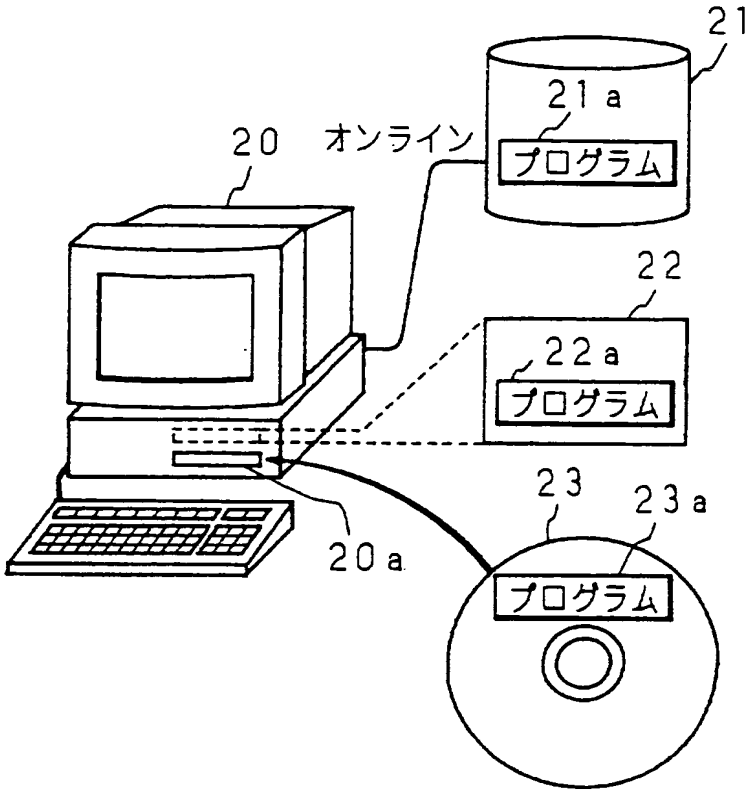
【図１】



【図２】

クラス1	クラス2	…	クラスK
$b_1 v_1^{(1)}$	$b_1 b_2 v_2^{(1)}$	…	$b_1 b_2 \cdots b_K v_K^{(1)}$
$b_1 v_1^{(2)}$	$b_1 b_2 v_2^{(2)}$	…	$b_1 b_2 \cdots b_K v_K^{(2)}$
⋮	⋮		⋮
$b_1 v_1^{(J)}$	$b_1 b_2 v_2^{(J)}$	…	$b_1 b_2 \cdots b_K v_K^{(J)}$

【図３】



【書類名】　　要約書

【要約】

【課題】　圧倒的多数の公開鍵の組合せから１つの公開鍵の組を任意に選択することに安全性の根拠を置いた新しいタイプの公開鍵暗号系の暗号化方法を提供する。

【解決手段】　各分割平文毎に乱数項を組み込んだ複数の公開鍵を予めデータベース10内に準備しておき、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文について選択し、選択した公開鍵を使用して暗号文Ｃを作成する。安全性の根拠を、多数の公開鍵から所望の公開鍵の組を自由に選択できること、言い換えれば、その公開鍵選択の組合せの数の多さに置いている。

【選択図】　　図１